The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
2011-09-13

SUBJECT:
Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS11-072)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Office Excel, a spreadsheet application. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Microsoft Office SharePoint Server 2007
- Microsoft Office 2010
- Microsoft Office 2007
- Microsoft Office 2003
- Microsoft Office 2011 for Mac
- Microsoft Office 2008 for Mac
- Microsoft Office 2004 for Mac
- Open XML File Format Converter for Mac
- Microsoft Works 9
- Microsoft Excel Viewer
- Microsoft Office Web Apps 2010

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Five privately reported vulnerabilities have been identified in Microsoft Excel that could allow remote code execution. These vulnerabilities are due to the way in which Microsoft Excel handles the following conditions while opening specially crafted Excel files:

- Out of Bounds Array Indexing

- Conditional Expression Parsing
- Use after Free WriteAV
- Heap Corruption

These vulnerabilities can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Excel file as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted Excel file that is hosted on the page.

RECOMMENDATIONS:

The following actions should be taken:

· Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

· Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

· Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

· Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

· Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:

http://technet.microsoftcom/en-us/security/bulletin/ms11-072
http://support.microsoft.com/kb/2587505

SecurityFocus:

http://www.securityfocus.com/bid/49477

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1986
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1987
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1988
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1989
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1990